Specification features in selected application scenarios

UNDERSTANDING WS-FEDERATION

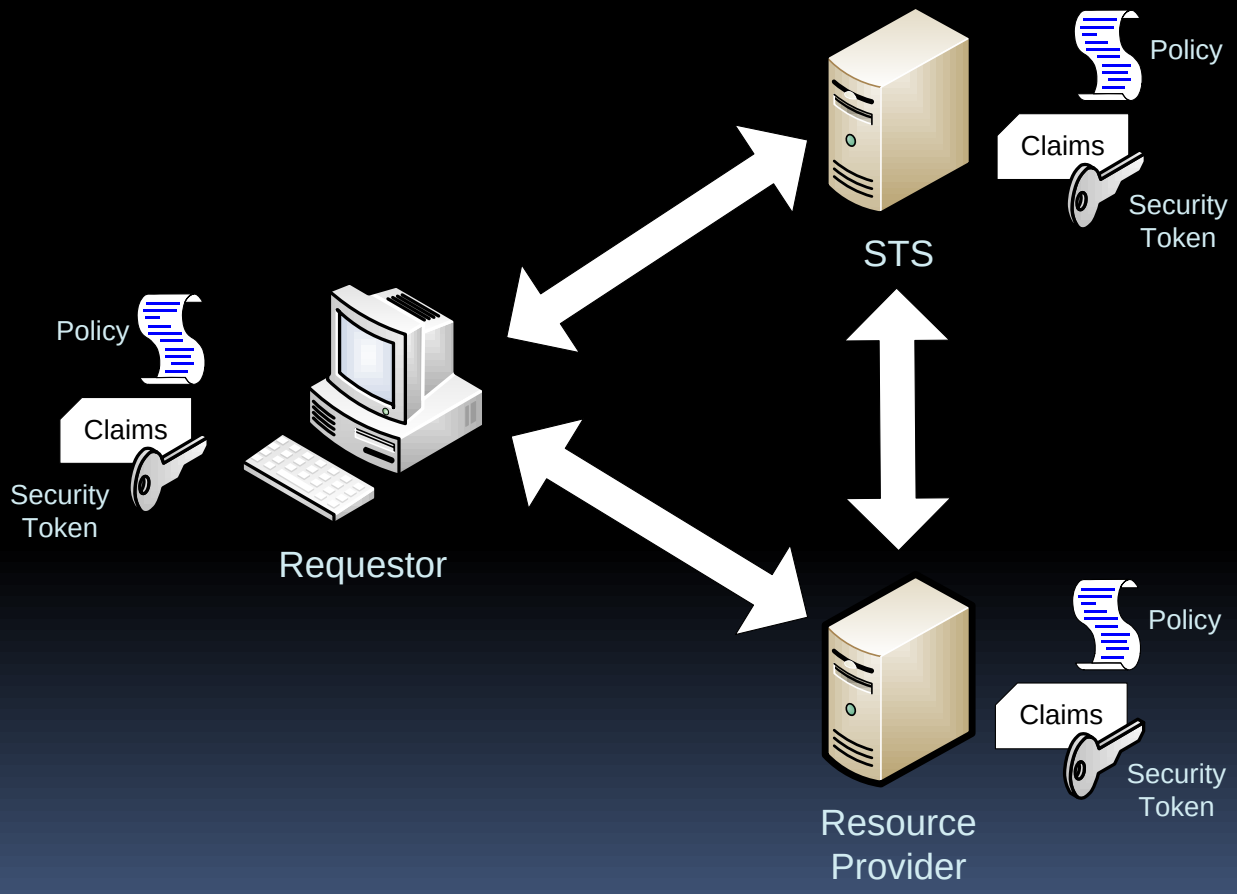
Agenda

- WS-Trust and WS-Federation Fundamentals
- Enterprise Scenario – Request for Proposal
- Healthcare Scenario – Patient Record Access

WS-Trust

- Defines Security Token Service (STS) model for security tokens including
  - Requesting
  - Issuing
  - Renewing
  - Cancelling
  - Validating
- Token type agnostic

The STS Model



WS-Federation

- Enables richer trust relationships
- Allows authorized access to resources in one realm provided to security principles managed in another
- Defines mechanisms as extensions to WS-Trust for:
  - Brokering of identity
  - Attribute discovery and retrieval
  - Authentication and authorization claims between federation partners
  - Protection of the privacy of claims across organizational boundaries
- Provides for mapping of the above, and WS-Trust token issuance messages, onto HTTP for web browser clients

Enterprise scenario

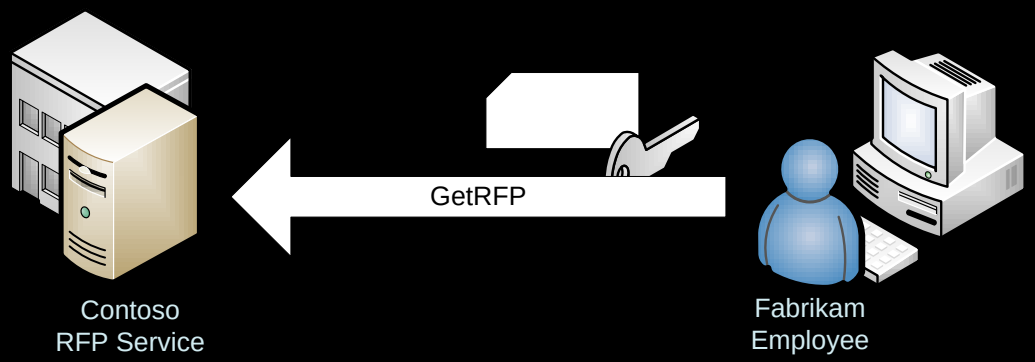
- Request for Proposal
  - First interaction between new business partners
  - Simple review, bid and status check for RFPs
- WS-Federation features demonstrated:
  - Federation Metadata
  - Application specific Policy and Metadata
  - Authorization Context
  - Common Claim Types
  - Web Browser Requestors

Initial RFP Request

Fabrikam is new partner of Contoso

Fabrikam Employee initiates first request to get available RFPs from the Contoso service

Request is secured by a token signed with Fabrikam's signing key



Contoso attempts to authenticate the request but finds that additional configuration is needed because this is the first time the two have worked together

Request is put on hold

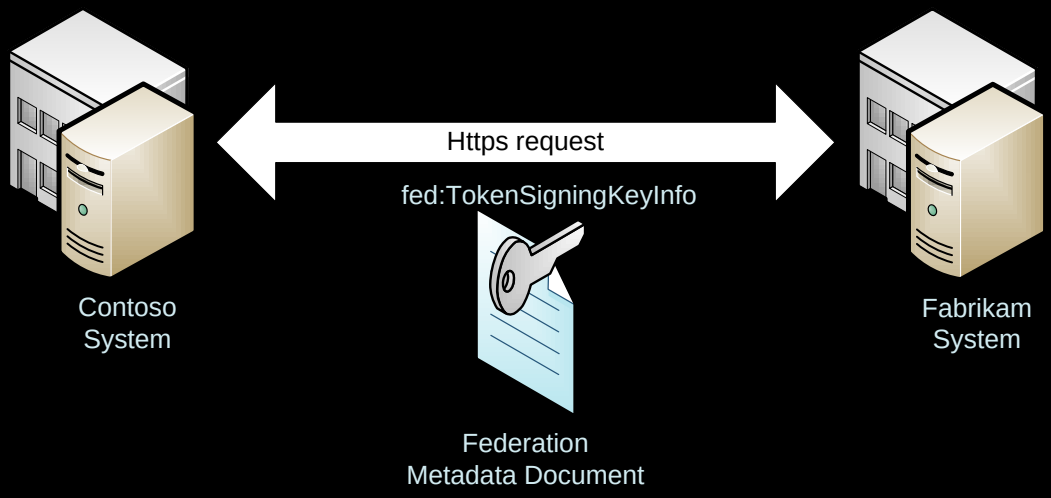
Federation Configuration

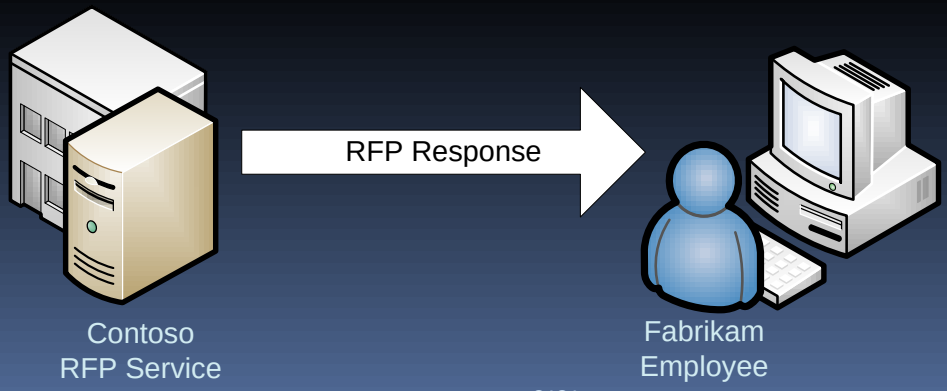
Contoso algorithmically constructs endpoint to retrieve Fabrikam's Federation Metadata Document

This contains Fabrikam's signing key as well as additional information, (e.g. supported claim types)

Contoso's system configures itself and can now authenticate requests from Fabrikam

The held request is authenticated and a response is returned





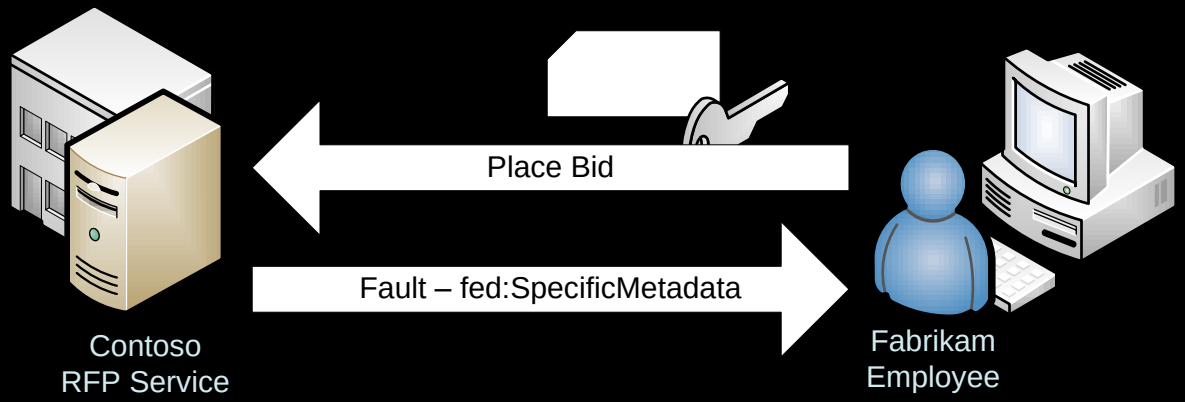
Specific Metadata Required

A Fabrikam employee submits a bid to the Contoso service

*Only Bonded Employees are authorized to submit bids

A specialized SOAP fault is returned indicating the specific policy and metadata required to process this request.

The claim type is expressed using the Common Claims Dialect



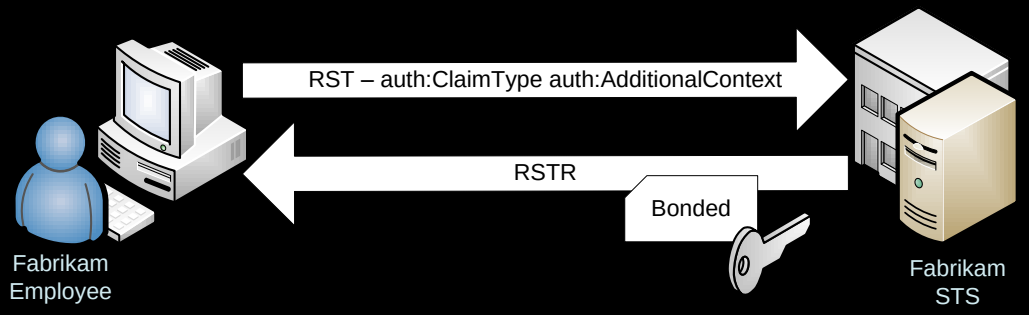

```
<wst:Claims  Dialect="…/authorization/authclaims">
  <auth:ClaimType Uri="…/claims/Group">
    <auth:Value>Bonded</auth:Value>
  </auth:ClaimType>
</wst:Claims>
```

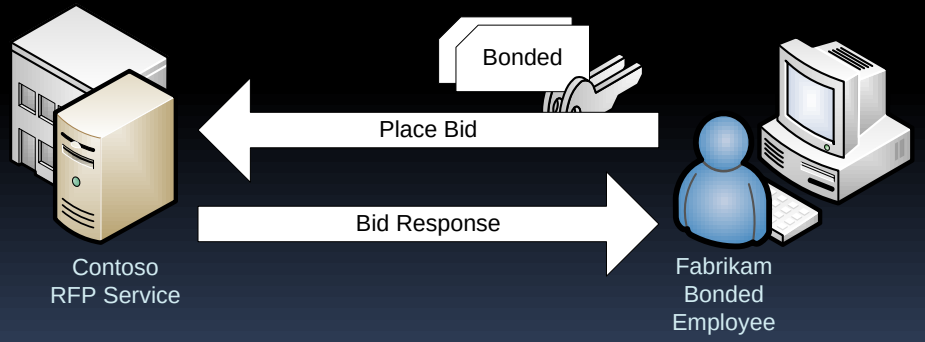
Authorization Context

The Fabrikam client issues a request to the Fabrikam STS for the required claims

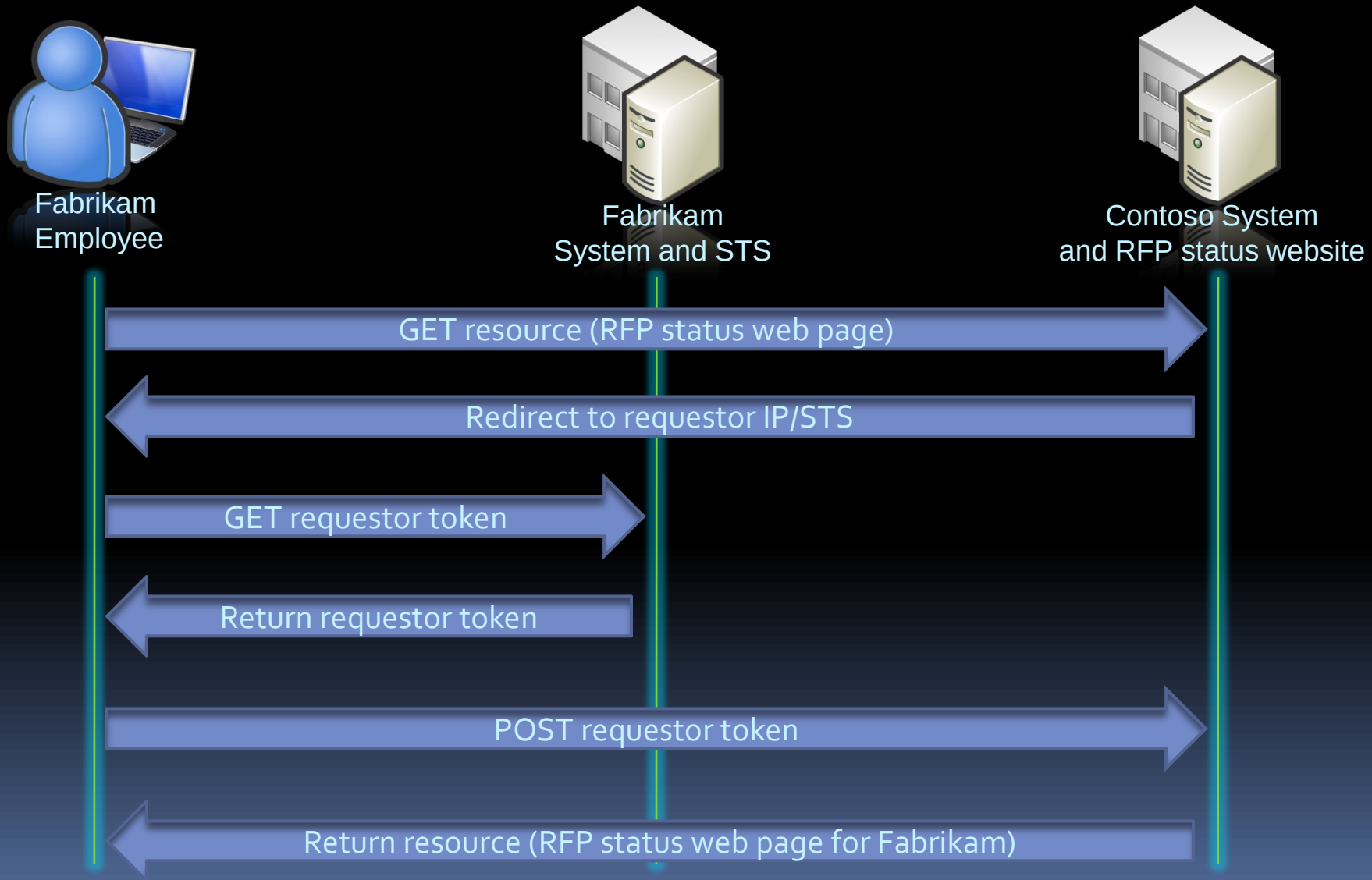
The Fabrikam client provides additional context for the request via WS-Federation's Authorization Context

The Fabrikam client resubmits the bid with the original token and the new token to the Contoso RFP service

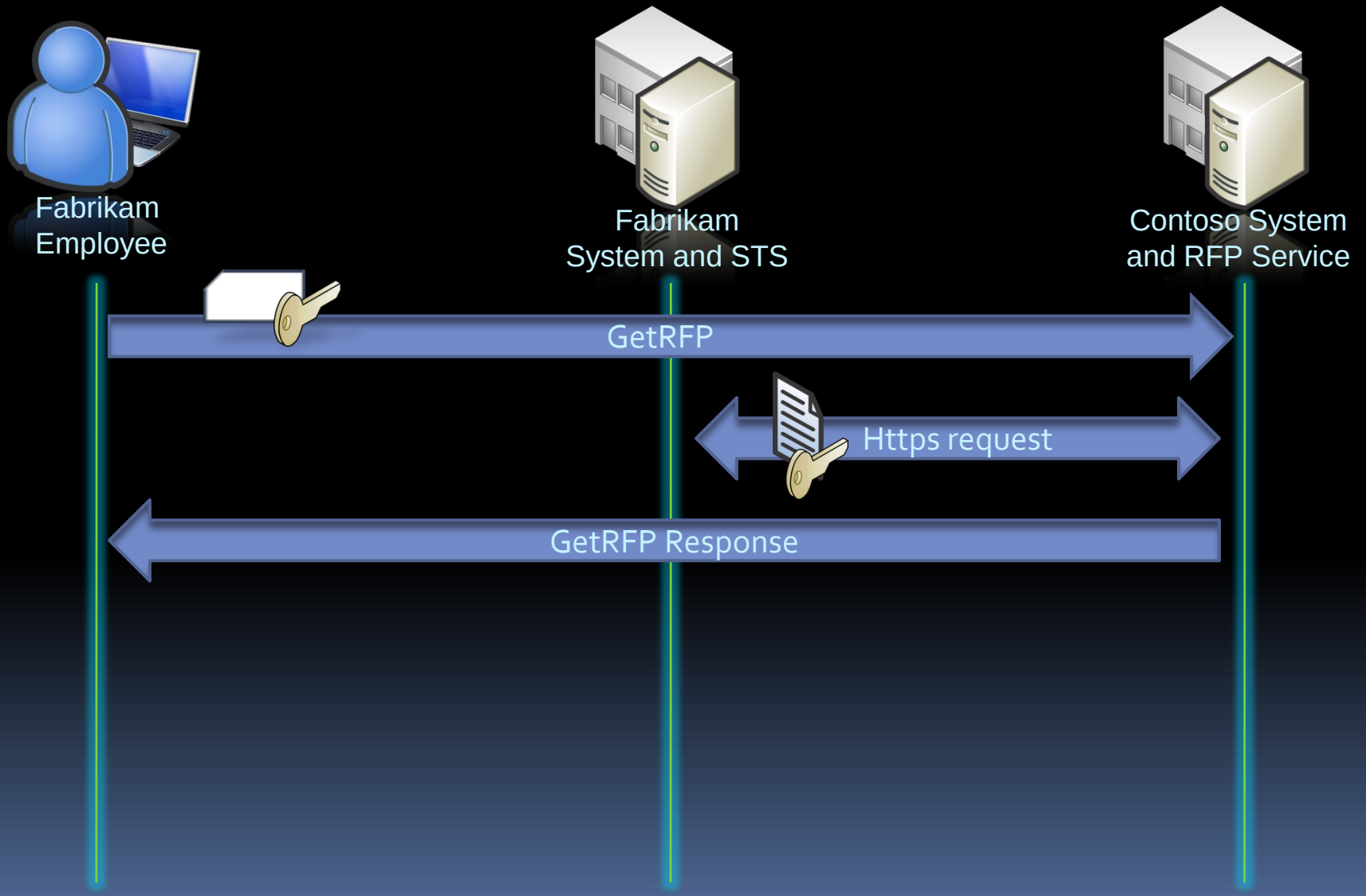




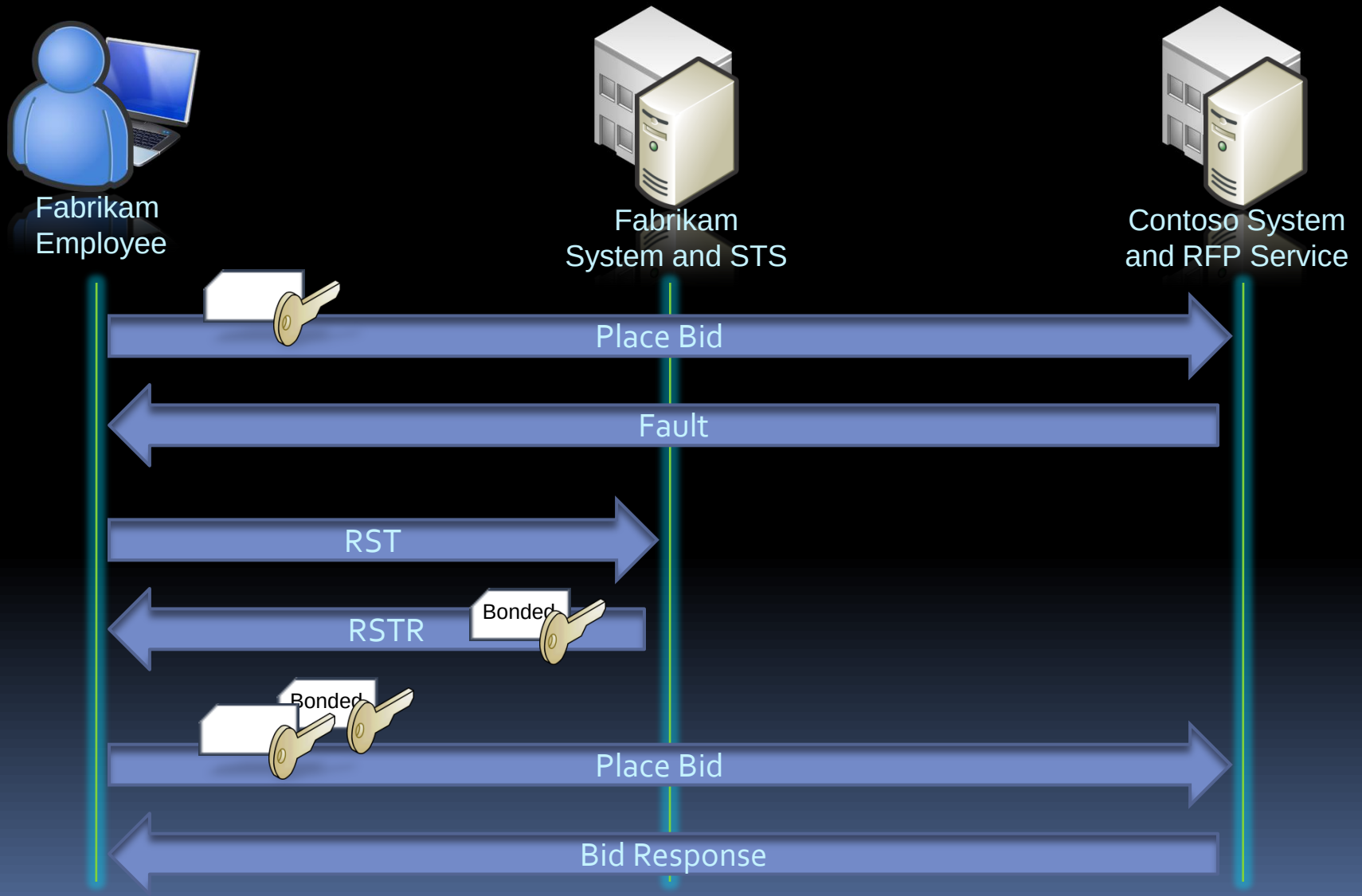
Enterprise web requestor



Complete Enterprise Scenario



Complete Enterprise Scenario



Enterprise Scenario Review

- Federation Metadata
  - Automated configuration between Contoso and Fabrikam
- Application specific Policy and Metadata
  - Indicated specific claim required
- Authorization Context
  - Provided additional context for token request
- Common Claim Types
  - Used to express required claims
- Web Browser Requestors
  - Review bid status web page

Healthcare Scenario

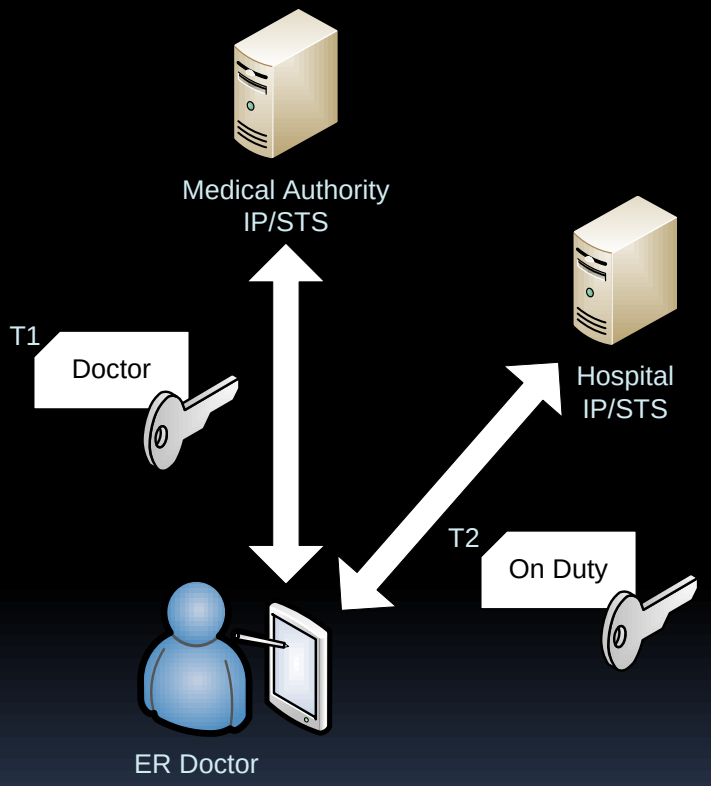
- Patient Record Access
  - Emergency health record requested for an unconscious patient
  - Multiple organizational boundaries crossed
- WS-Federation Features
  - Federation Metadata
  - Application specific Policy and Metadata
  - Authorization Context
  - Privacy Protection
  - Sign Out

ER Doctor Signs In

The scenario begins with an ER Doctor who starts a shift and signs into an application.

An STS of a certifying Medical Authority issues a token containing claims that the ER Doctor is a licensed physician

The Hospital STS issues a token with claims that the ER Doctor is on duty.



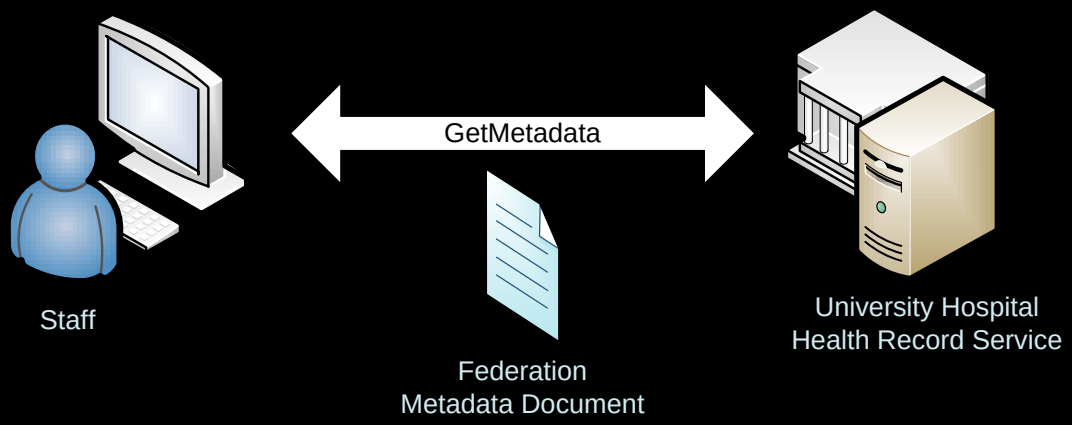
Health Record Service Discovery

An unconscious patient arrives at the ER

The patient has a student ID card with a link to an affiliated University Hospital Health Record Service

Hospital staff enter the link into their system which retrieves endpoints and metadata from the University Hospital

Federation Metadata Document is returned with specific access requirements

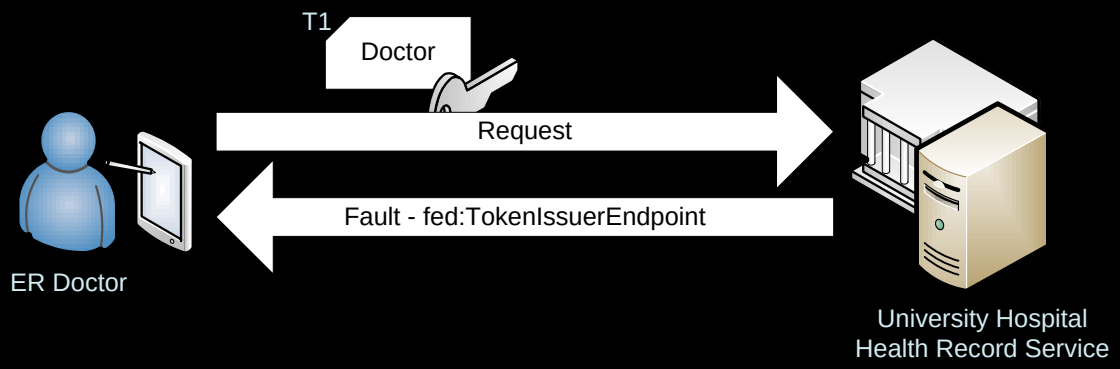


Specific Policy and Metadata

ER Doctor chooses the emergency access option which requires a token with claims from the Medical Authority that are satisfied by T1

A fault is returned that indicates an additional token is required from the patient's Primary Care Provider

The fault also contains Authorization Context information to pass on to assist the Primary Care Provider in processing the request for the token

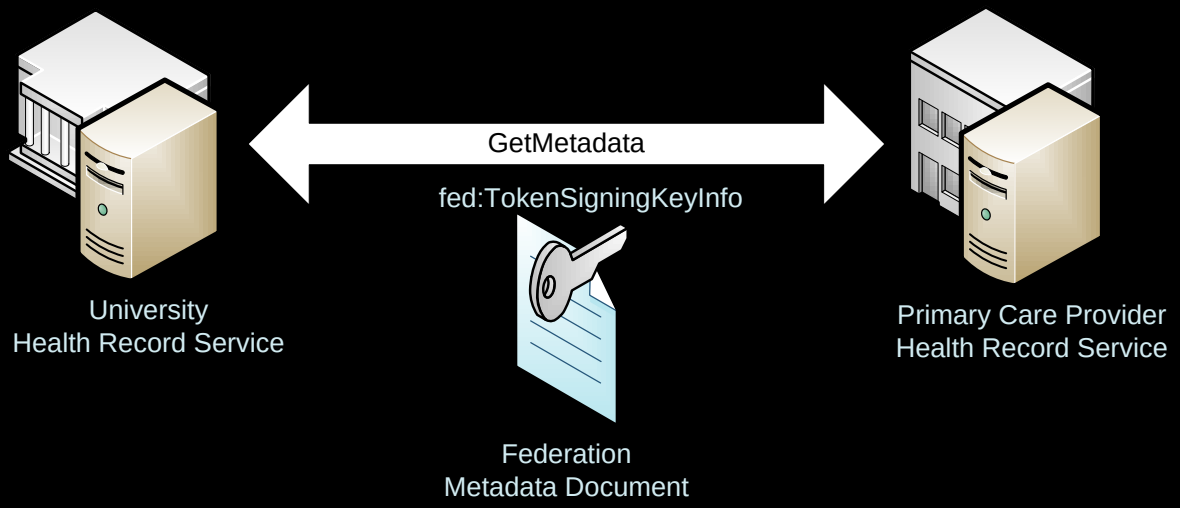



```
<sp:RequestSecurityTokenTemplate>
  <auth:AdditionalContext>
    <auth:ContextItem Name=".../AccessReq">
      <auth:Value>...</auth:Value>
    </auth:ContextItem>
  </auth:AdditionalContext>
</sp:RequestSecurityTokenTemplate>
```

Patient Selected Delegate

In a normal case the request for patient records would have been successful

In this case, the patient upon enrolling with the University Hospital insurance program indicated their Primary Care Physician as a delegate to release records rather than allow any certified doctor access



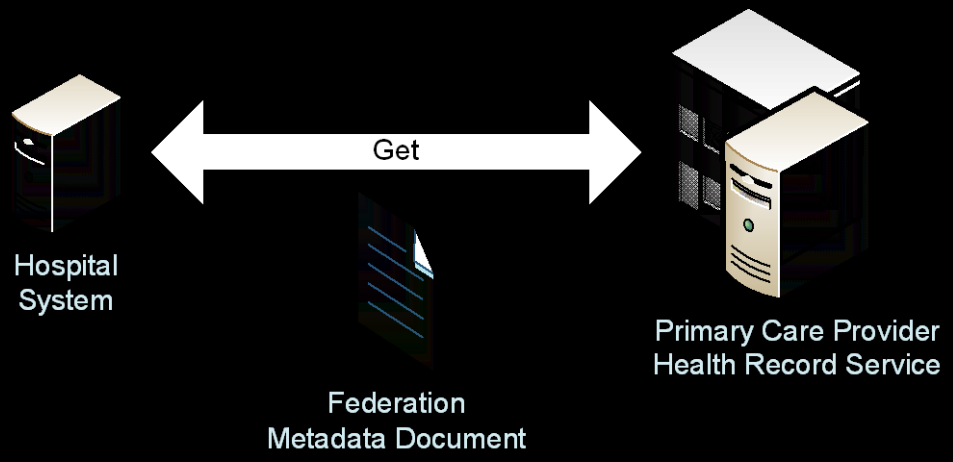
The University Hospital and the Primary Care Physician then entered into a federation to share signing keys, claims, etc.

Acquiring the Missing Token

The Hospital client acquires the interface and metadata of the Primary Care Provider STS

Included within the Federation Metadata Document are the offered claim types of the service

One of the claim types understood by the Hospital client is one it does not want exposure to if it is issued



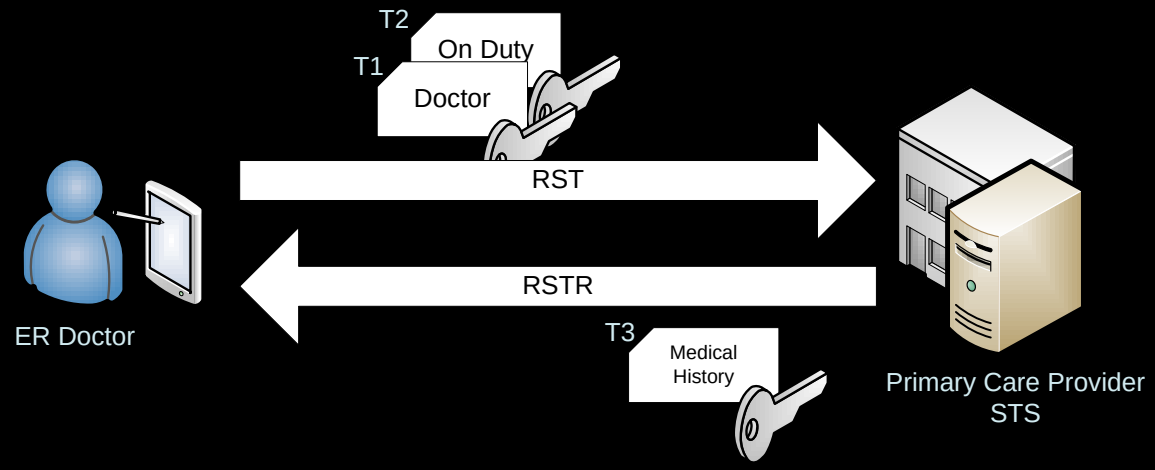

```
<fed:UriNamedClaimTypesOffered>
  <fed:ClaimType Uri=".../PsychiatricHistory">
    <fed:DisplayName>
      Psychiatric History Record Locator
    </fed:DisplayName>
  </fed:ClaimType>
  <fed:ClaimType Uri=".../MedicalHistory">
    <fed:DisplayName>
      Medical History Record Locator
    </fed:DisplayName>
  </fed:ClaimType>
</fed:UriNamedClaimTypesOffered>
```

Requesting the Missing Token

Two tokens are required for authenticating a request for the missing token T3 that are satisfied by T1 and T2

This is a more stringent requirement for access to the patient records than the University Hospital's requirements

The RST from the Hospital Client indicates the claim it does not want exposure to should be protected using Privacy Confidential Tokens feature, presumably so that only the PCP and the University Hospital can access it

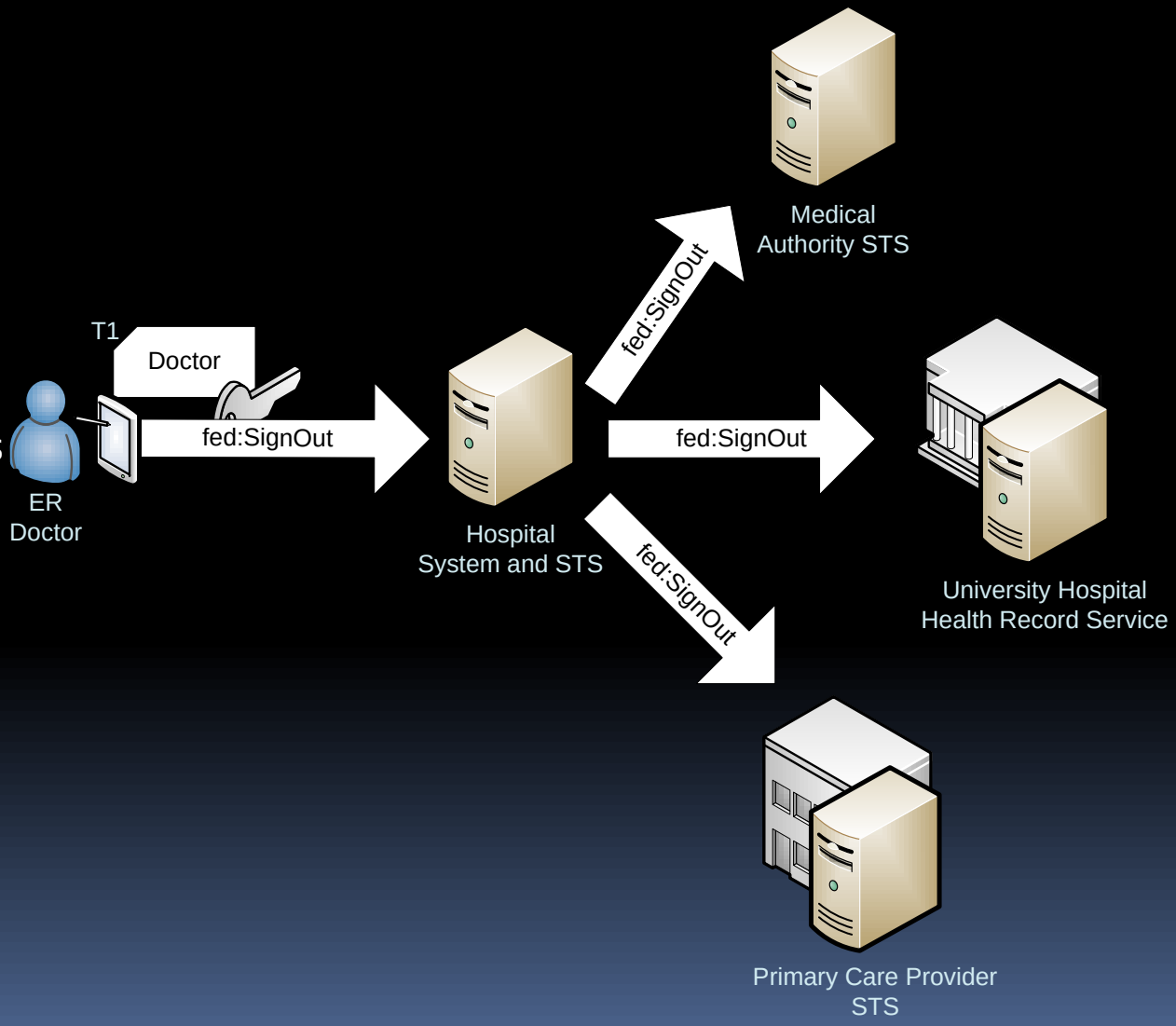



```
<priv:ProtectData>
  <wst:Claims Dialect=".../authorization/authclaims">
    <auth:ClaimType Uri=".../PsychiatricHistory"/>
  </wst:Claims>
</priv:ProtectData>
```

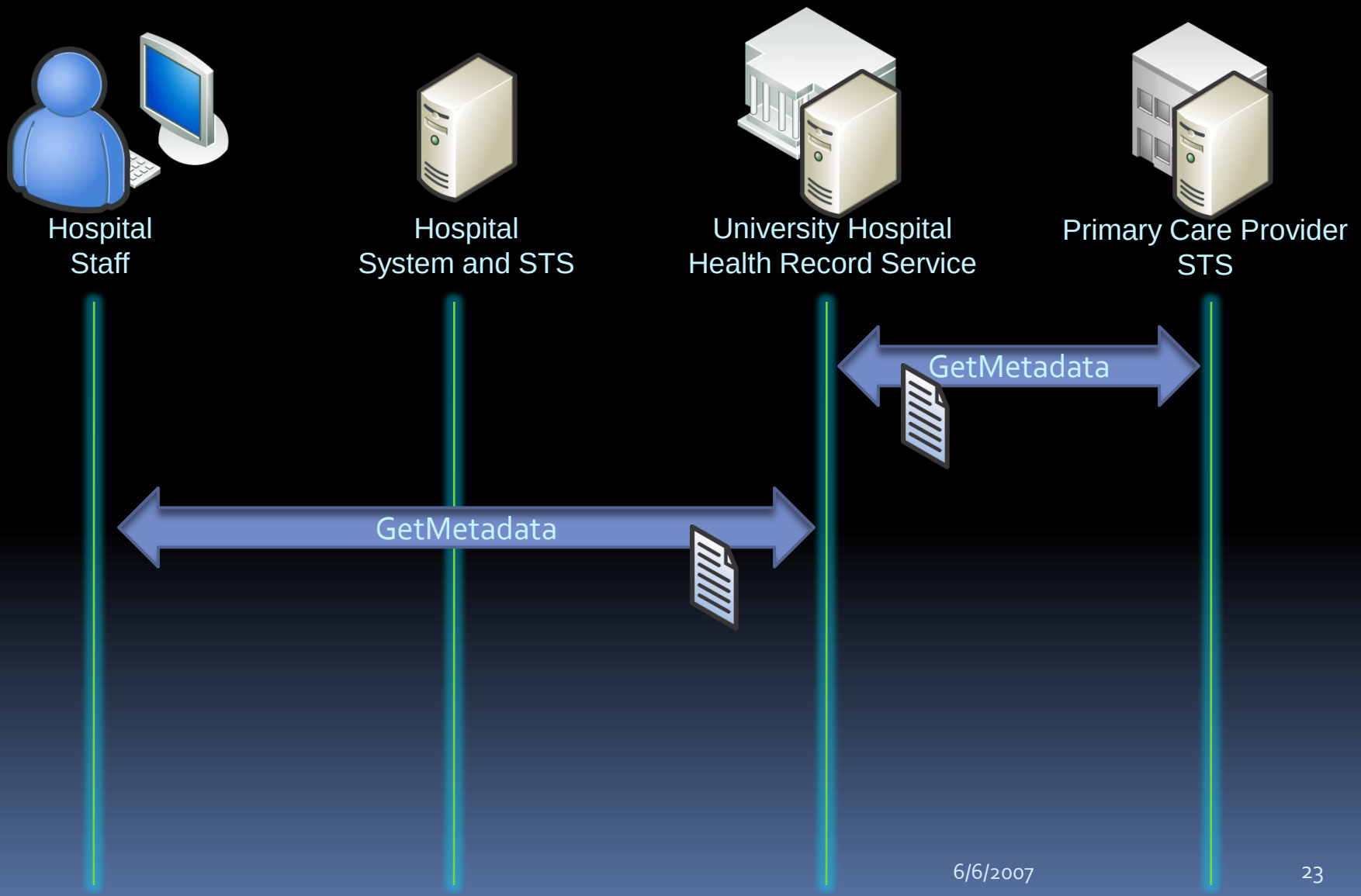
Sign out

The ER Doctor logs out of the Hospital application at the end of the day

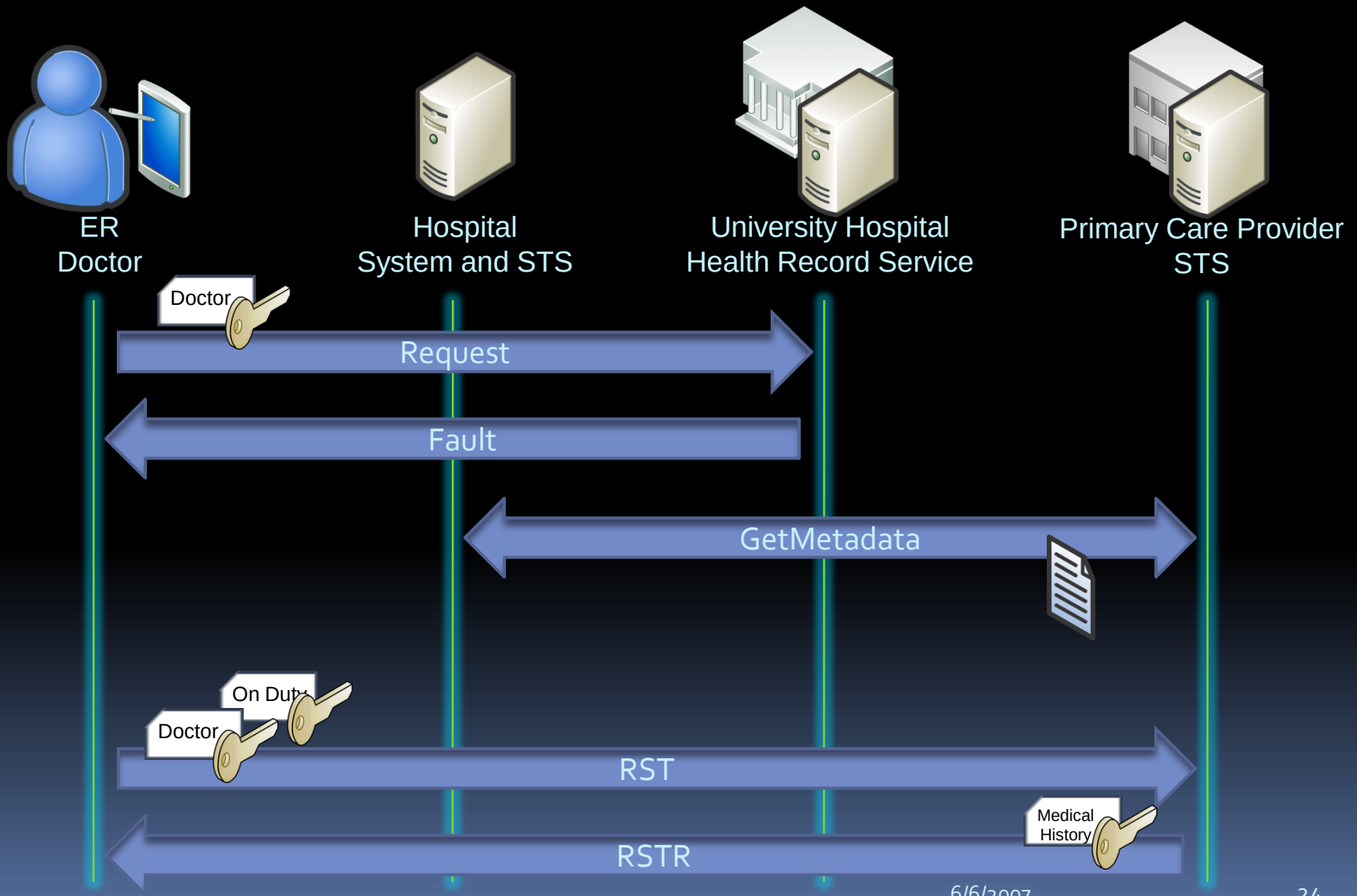
A SignOut message is sent to each of the endpoints, which the Hospital application has tracked throughout the day, so that unneeded endpoint states can be cleaned up.



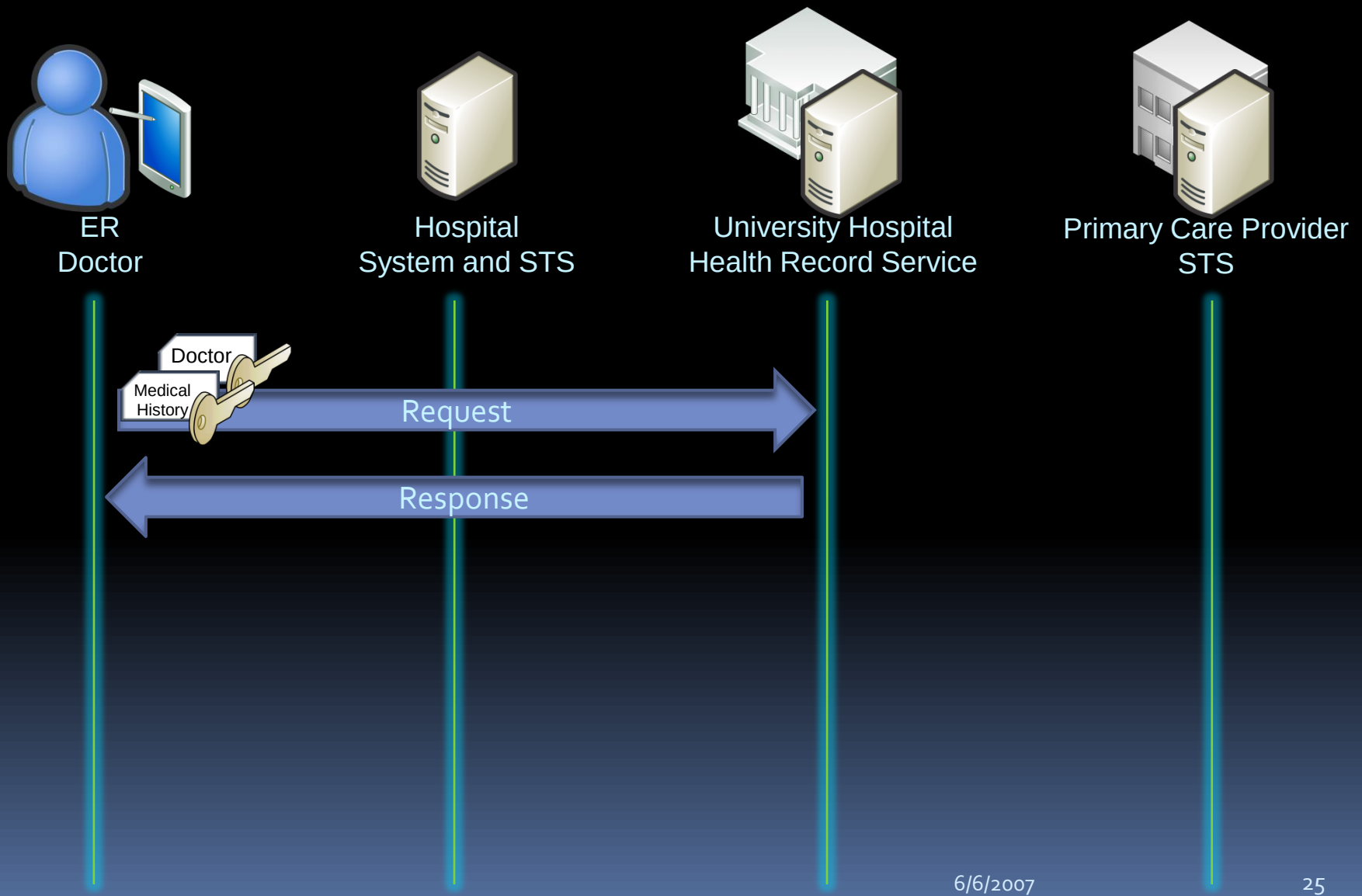
Complete Healthcare Scenario



Complete Healthcare Scenario



Complete Healthcare Scenario



Healthcare Scenario Review

- Federation Metadata
  - Used in configuration between participants
  - Use of Token Issuer, Authorization Context and Offered Claims shown
- Application specific Policy and Metadata
  - Shown use when additional token and issuer required
- Authorization Context
  - Shown in use from a Relying Party to assist STS in making authorization decision
- Privacy Protection
  - Used by Hospital client to avoid possible exposure to sensitive claim
- Sign Out
  - Cleans up state for tokens issued that are no longer required

Review

- WS-Trust STS Model and WS-Federation
- Scenarios
  - Enterprise – Request For Proposal
  - Healthcare – Patient Record Access
- WS-Federation features shown
  - Federation Metadata
  - Application specific Policy and Metadata
  - Authorization Context
  - Common Claim Types
  - Privacy Protection
  - Sign Out
  - Web Browser Requestors